

ON THE NUMBER OF RAMIFIED PRIMES IN SPECIALIZATIONS OF FUNCTION FIELDS OVER \mathbb{Q}

LIOR BARY-SOROKER AND FRANÇOIS LEGRAND

ABSTRACT. We study the number of ramified prime numbers in finite Galois extensions of \mathbb{Q} obtained by specializing a finite Galois extension of $\mathbb{Q}(T)$. Our main result is a central limit theorem for this number. We also give some Galois theoretical applications.

1. INTRODUCTION

Given an indeterminate T , the *specialization* of a finite Galois extension $E/\mathbb{Q}(T)$ with Galois group G at a point $t_0 \in \mathbb{P}^1(\mathbb{Q})$, which is not a branch point, is a finite Galois extension of \mathbb{Q} whose Galois group is a subgroup of G ; we denote it by E_{t_0}/\mathbb{Q} (see §2.1 for basic terminology). For example, if E is the splitting field over $\mathbb{Q}(T)$ of a monic polynomial $P(T, Y) \in \mathbb{Q}[T][Y]$ which is separable in Y , then E_{t_0} is the splitting field over \mathbb{Q} of $P(t_0, Y)$ (for all but finitely many $t_0 \in \mathbb{Q}$).

1.1. The arithmetic function $\text{Ram}_{E/\mathbb{Q}(T)}$. In this paper, we are interested in the number of prime numbers ramifying in finite Galois extensions of \mathbb{Q} obtained by specializing a finite Galois extension of $\mathbb{Q}(T)$ at positive integers. More precisely, let us define:

Definition 1.1. Let $E/\mathbb{Q}(T)$ be a finite Galois extension. Given a positive integer n which is not a branch point, let

$$\text{Ram}_{E/\mathbb{Q}(T)}(n)$$

be the number of ramified prime numbers in the specialization E_n/\mathbb{Q} . If n is a branch point, we set arbitrarily $\text{Ram}_{E/\mathbb{Q}(T)}(n) = -1$.

Note that $\text{Ram}_{E/\mathbb{Q}(T)}$ depends on the choice of the indeterminate T .

Remark 1.2. If $E/\mathbb{Q}(T)$ is trivial over $\overline{\mathbb{Q}}^1$, then there are no branch points and the extension E_{t_0}/\mathbb{Q} does not depend on t_0 . In particular, the function $\text{Ram}_{E/\mathbb{Q}(T)}$ is constant. *From now on, we tactically assume throughout this paper that the extension $E/\mathbb{Q}(T)$ is not trivial over $\overline{\mathbb{Q}}$.*

Date: November 10, 2015.

¹*i.e.* the compositum of E and $\overline{\mathbb{Q}}(T)$ (in a given algebraic closure of $\mathbb{Q}(T)$) is equal to $\overline{\mathbb{Q}}(T)$ or, equivalently, if there exists a number field F such that $E = F(T)$.

Some properties of the function $\text{Ram}_{E/\mathbb{Q}(T)}$ can be derived from results in the literature. For example, it is unbounded. More precisely, the second author [Leg13], [Leg14] proves that, given a finite Galois extension $E/\mathbb{Q}(T)$ with Galois group G and a finite set \mathcal{S} of sufficiently large suitable prime numbers (depending on the extension $E/\mathbb{Q}(T)$), there exist infinitely many positive integers n such that the specialization of $E/\mathbb{Q}(T)$ at n has Galois group G and ramifies at each prime number of \mathcal{S} ². In particular, given a positive integer m , there exist infinitely many positive integers n such that $\text{Gal}(E_n/\mathbb{Q}) = G$ and $\text{Ram}_{E/\mathbb{Q}(T)}(n) \geq m$.

On the other hand, the first author and Schlank [BSS] prove that the function $\text{Ram}_{E/\mathbb{Q}(T)}$ does not tend to ∞ . Furthermore, several works consist in producing, for some finite groups G and some specific finite Galois extensions $E/\mathbb{Q}(T)$ with Galois group G , some positive integers n such that the specialization E_n/\mathbb{Q} has Galois group G and the number $\text{Ram}_{E/\mathbb{Q}(T)}(n)$ is small; see *e.g.* [JR03], [MR05], [JR07], [Rob11] and [BSS]. For example, for $G = S_N$ ($N \geq 3$) and some specific realizations over $\mathbb{Q}(T)$ of S_N with 3 branch points, one has $\text{Ram}_{E/\mathbb{Q}(T)}(n) \leq 3$ for infinitely many positive integers n ; see [BSS].

1.2. Main result. We study the statistical properties of the arithmetic function $\text{Ram}_{E/\mathbb{Q}(T)}$ for a given finite Galois extension $E/\mathbb{Q}(T)$.

Recall that the absolute Galois group of \mathbb{Q} acts on the branch points of the extension $E/\mathbb{Q}(T)$ lying in $\overline{\mathbb{Q}}$ (*i.e.* which are different from ∞). Let r be the number of orbits under this action. By the Riemann-Hurwitz formula, one has $r \geq 1$ (as the extension $E/\mathbb{Q}(T)$ has been assumed not to be trivial over $\overline{\mathbb{Q}}$; see remark 1.2).

Theorem 1.3. *For each positive integer k , one has*

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{0 < n \leq N} \left(\frac{\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{-\frac{t^2}{2}} dt.$$

Although $\text{Ram}_{E/\mathbb{Q}(T)}$ depends on the choice of T , the limit distribution of the normalization of $\text{Ram}_{E/\mathbb{Q}(T)}$ given in theorem 1.3 does not.

Taking $k = 1$ and $k = 2$ in theorem 1.3 gives the following:

$$\begin{aligned} \frac{1}{N} \sum_{0 < n \leq N} \text{Ram}_{E/\mathbb{Q}(T)}(n) &\sim r \log \log(N), \quad N \rightarrow \infty, \\ \frac{1}{N} \sum_{0 < n \leq N} (\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N))^2 &\sim r \log \log(N), \quad N \rightarrow \infty. \end{aligned}$$

²Actually the inertia groups at prime numbers in \mathcal{S} in the specializations can be prescribed and explicit bounds on their discriminants are given.

Moreover, by the method of moments (see *e.g.* [Bil95, example 30.1 and theorem 30.2]), theorem 1.3 provides the limit distribution of our normalization of $\text{Ram}_{E/\mathbb{Q}(T)}$.

For every real number a , set

$$I(a) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^a e^{\frac{-t^2}{2}} dt.$$

Theorem 1.4. *For every real number a , one has*

$$\lim_{N \rightarrow \infty} \frac{1}{N} \left| \left\{ 0 < n \leq N : \frac{\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \leq a \right\} \right| = I(a).$$

Similar results hold for finite extensions $E/\mathbb{Q}(T)$ which are not necessarily Galois since, in this case, $\text{Ram}_{E/\mathbb{Q}(T)} = \text{Ram}_{\widehat{E}/\mathbb{Q}(T)}$ with \widehat{E} the Galois closure of E over $\mathbb{Q}(T)$ (see §5).

1.3. Applications. Below we give three corollaries of theorem 1.3 (see §3 for the proofs).

1.3.1. Application to inverse Galois theory. A classical motivation to study specializations of finite Galois extensions of $\mathbb{Q}(T)$ is the *inverse Galois problem*: does every finite group G occur as the Galois group of a Galois extension of \mathbb{Q} ? Indeed, a way to realize G is by specializing a Galois extension $E/\mathbb{Q}(T)$ with Galois group G : from the *Hilbert irreducibility theorem*, there exist infinitely many positive integers n which each satisfies the *Hilbert specialization property*, *i.e.* such that the specialization E_n/\mathbb{Q} still has Galois group G . Many finite groups have been shown to occur as a Galois group over \mathbb{Q} by this method; we refer to [MM99] for more details and references and [Zyw14] for more recent results.

We show that theorem 1.3 still holds if we restrict to the set of positive integral specialization points which satisfy the *Hilbert specialization property*.

Corollary 1.5. *Denote the Galois group of the extension $E/\mathbb{Q}(T)$ by G . Then, for each positive integer k , one has*

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{\substack{0 < n \leq N \\ \text{Gal}(E_n/\mathbb{Q})=G}} \left(\frac{\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{\frac{-t^2}{2}} dt.$$

Taking $k = 1$ in corollary 1.5 gives the following:

$$\frac{1}{N} \sum_{\substack{0 < n \leq N \\ \text{Gal}(E_n/\mathbb{Q})=G}} \text{Ram}_{E/\mathbb{Q}(T)}(n) \sim r \log \log(N), \quad N \rightarrow \infty.$$

Hence we reobtain that, given an integer $m \geq 1$, there exist integers $n \geq 1$ such that $\text{Gal}(E_n/\mathbb{Q}) = G$ and $\text{Ram}_{E/\mathbb{Q}(T)}(n) \geq m$. In particular, if a given non-trivial finite group G occurs as the Galois group of a finite Galois extension of $\mathbb{Q}(T)$ which is not trivial over $\overline{\mathbb{Q}}$, then, *given a positive integer m , there exists a finite Galois extension of \mathbb{Q} with Galois group G and at least m ramified prime numbers*. We notice that, for some Galois groups over \mathbb{Q} , the latter condition has not been proved yet. For example, there exist odd prime numbers p for which all known realizations of $\text{PSL}_2(\mathbb{F}_p)$ over \mathbb{Q} ramify only at 2 and p [Zyw13].

1.3.2. *Two corollaries on the function $\text{Ram}_{E/\mathbb{Q}(T)}$.* From theorem 1.3 with $k = 2$, we get a normal order of the function $\text{Ram}_{E/\mathbb{Q}(T)}$:

Corollary 1.6. *Let $\epsilon > 0$. Then, for each positive integer n which is not in some set S_ϵ which has asymptotic density zero, one has*

$$(1 - \epsilon) \cdot r \log \log(n) \leq \text{Ram}_{E/\mathbb{Q}(T)}(n) \leq (1 + \epsilon) \cdot r \log \log(n).$$

Consequently, the set of all positive integers n such that $\text{Ram}_{E/\mathbb{Q}(T)}(n) \leq C$ for a given non-negative integer C has asymptotic density zero. The following corollary, which rests on theorem 1.3 with arbitrary k , gives upper bounds on the rate of convergence.

Corollary 1.7. *Let C and k be two non-negative integers with $k \geq 1$. Then there are some positive constants $\alpha(k, r)$ and $A(C, k, r)$ such that*

$$\frac{1}{N} \left| \left\{ 0 < n \leq N : \text{Ram}_{E/\mathbb{Q}(T)}(n) \leq C \right\} \right| \leq \frac{\alpha(k, r)}{\log \log(N)^k}$$

for each positive integer $N \geq A(C, k, r)$.

1.4. **Summary of the proof of theorem 1.3.** The proof, given in §4, has two parts that we summarize below. Let $P_E(T) \in \mathbb{Z}[T]$ be a separable polynomial whose roots are the finite branch points of $E/\mathbb{Q}(T)$.

First, given a positive integer n which is not a branch point of the extension $E/\mathbb{Q}(T)$, we relate the number $\text{Ram}_{E/\mathbb{Q}(T)}(n)$ to the number $\omega(P_E(n))$ of distinct prime numbers dividing $P_E(n)$ (without multiplicity). Namely, we make the difference

$$\text{Ram}_{E/\mathbb{Q}(T)}(n) - \omega(P_E(n))$$

completely explicit up to $O(1)$ (lemma 4.4). This step is based on the use of a classical result about ramification in specializations [Bec91], [Leg14, §2.2] (see lemma 4.2) and of some generalized version of the arithmetic function ω (definition 4.3).

Next, we study this prime divisor counting function (lemma 4.5) and then show that the difference $\text{Ram}_{E/\mathbb{Q}(T)}(n) - \omega(P_E(n))$ is negligible in

our context. Namely, for each positive integer k , we show that

$$(1) \quad \sum_{0 < n \leq N} \left(\text{Ram}_{E/\mathbb{Q}(T)}(n) - \omega(P_E(n)) \right)^k = O(N)$$

as N tends to ∞ (lemma 4.6). By a result of Halberstam [Hal56, theorem 4], one has

$$(2) \quad \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{0 < n \leq N} \left(\frac{\omega(P_E(n)) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{-\frac{t^2}{2}} dt.$$

Conjoining (1) and (2) then provides theorem 1.3.

Acknowledgments. We wish to thank Pierre Dèbes, Steve Lester and Zéev Rudnick for helpful discussions and valuable comments. The first author is partially supported by the Israel Science Foundation (grant No. 40/14). The second author is partially supported by the Israel Science Foundation (grants No. 40/14 and No. 696/13).

2. PRELIMINARIES AND NOTATION

2.1. Preliminaries. Let T be an indeterminate and $E/\mathbb{Q}(T)$ a finite Galois extension, assumed not to be trivial over $\overline{\mathbb{Q}}$.

A point $t_0 \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is a *branch point* of $E/\mathbb{Q}(T)$ if the prime ideal $(T - t_0) \overline{\mathbb{Q}}[T - t_0]$ ³ ramifies in the integral closure of $\overline{\mathbb{Q}}[T - t_0]$ in the *compositum* of E and $\overline{\mathbb{Q}}(T)$ (in a fixed algebraic closure of $\mathbb{Q}(T)$). The extension $E/\mathbb{Q}(T)$ has only finitely many branch points and their number is positive (actually at least 2); see remark 1.2.

Given a point $t_0 \in \mathbb{P}^1(\mathbb{Q})$ which is not a branch point, the residue field of a prime ideal \mathcal{P} lying over $(T - t_0) \mathbb{Q}[T - t_0]$ in the extension $E/\mathbb{Q}(T)$ is denoted by E_{t_0} and we call the extension E_{t_0}/\mathbb{Q} the *specialization* of $E/\mathbb{Q}(T)$ at t_0 . This does not depend on the choice of the prime ideal \mathcal{P} lying over $(T - t_0) \mathbb{Q}[T - t_0]$ since $E/\mathbb{Q}(T)$ is Galois. The specialization E_{t_0}/\mathbb{Q} is a Galois extension of \mathbb{Q} whose Galois group is a subgroup of $\text{Gal}(E/\mathbb{Q}(T))$, namely the decomposition group of the extension $E/\mathbb{Q}(T)$ at \mathcal{P} .

2.2. Notation. The notation below will be used throughout the paper.

Let T be an indeterminate and $E/\mathbb{Q}(T)$ a finite Galois extension with Galois group G . Recall that the absolute Galois group of \mathbb{Q} acts on the branch points of the extension $E/\mathbb{Q}(T)$ lying in $\overline{\mathbb{Q}}$. Let $r \geq 1$ be the number of distinct orbits under this action and

$$(3) \quad \{t_1, \dots, t_r\}$$

³Replace $T - t_0$ by $1/T$ if $t_0 = \infty$.

a set of representatives. For each $i \in \{1, \dots, r\}$, denote the ramification index of $(T - t_i)\overline{\mathbb{Q}}[T - t_i]$ in $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ by

$$(4) \quad e_i$$

and let

$$(5) \quad P_i(T) \in \mathbb{Z}[T]$$

be the unique polynomial with positive leading coefficient b_i , which is irreducible over \mathbb{Z} and which satisfies $P_i(t_i) = 0$. Finally, set

$$(6) \quad P_E(T) = \prod_{i=1}^r P_i(T).$$

Denote by $\omega(n)$ the number of distinct prime divisors (without multiplicity) of a given positive integer n .

3. PROOFS OF COROLLARIES 1.5, 1.6 AND 1.7 ASSUMING THEOREM 1.3

3.1. Proof of corollary 1.5. We need first the following elementary bound. The lemma below will be used again in the last part of the proof of theorem 1.3 (§4.2).

Lemma 3.1. *One has $\text{Ram}_{E/\mathbb{Q}(T)}(n) = O(\log(n)/\log \log(n))$, $n \rightarrow \infty$.*

Proof. Let $P(T, Y) \in \mathbb{Z}[T][Y]$ be a monic separable (in Y) polynomial with splitting field E over $\mathbb{Q}(T)$ and $\Delta(T) \in \mathbb{Z}[T]$ its discriminant. For every integer n which is not a root of $\Delta(T)$, n is not branch point of $E/\mathbb{Q}(T)$, the field E_n is the splitting field over \mathbb{Q} of the polynomial $P(n, Y)$ and each prime number p which ramifies in the extension E_n/\mathbb{Q} divides $\Delta(n)$. Hence, from the classical bound

$$\omega(n) = O(\log(n)/\log \log(n)), \quad n \rightarrow \infty$$

(see e.g. [SMC06, §V.15]) and as $\Delta(n)$ is polynomial in n , one gets

$$\text{Ram}_{E/\mathbb{Q}(T)}(n) \leq \omega(\Delta(n)) = O(\log(n)/\log \log(n)), \quad n \rightarrow \infty,$$

as needed. \square

Proof of corollary 1.5. For any positive integers k and N , set

$$f_k(N) = \sum_{\substack{0 < n \leq N \\ \text{Gal}(E_n/\mathbb{Q}) < G}} \left(\frac{\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k.$$

By theorem 1.3, it suffices to show that $f_k(N) = o(N)$, $N \rightarrow \infty$, $k \geq 1$.

By lemma 3.1, one has $f_k(N) = O(g(N) \cdot \log^k(N) \cdot (\log \log(N))^{-k})$, $N \rightarrow \infty$, where $g(N)$ denotes the number of all positive integers $n \leq N$

such that $\text{Gal}(E_n/\mathbb{Q}) < G$. It then remains to use that $g(N) = O(\sqrt{N})$ as N tends to ∞ (see *e.g.* [Ser92, page 26]) to finish the proof. \square

3.2. Proof of corollary 1.6. Given a positive real number ϵ , let S_ϵ be the set of all positive integers n such that

$$|\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(n)| > \epsilon \cdot r \log \log(n).$$

Given a positive integer N , one has

$$\frac{|\{0 < n \leq N : n \in S_\epsilon\}|}{N} \leq \frac{1}{\sqrt{N}} + \frac{1}{N} \sum_{\substack{\sqrt{N} < n \leq N \\ n \in S_\epsilon}} 1.$$

Then, to get corollary 1.6, it suffices to prove

$$(7) \quad \frac{1}{N} \sum_{\substack{\sqrt{N} < n \leq N \\ n \in S_\epsilon}} 1 = o(1), \quad N \rightarrow \infty.$$

By the definition of the set S_ϵ , one has

$$(8) \quad \frac{1}{N} \sum_{\substack{\sqrt{N} < n \leq N \\ n \in S_\epsilon}} 1 < \frac{1}{N} \sum_{\sqrt{N} < n \leq N} \frac{(\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(n))^2}{\epsilon^2 \cdot (r \log \log(\sqrt{N}))^2}.$$

As $(A - B)^2 \leq 2A^2 + 2B^2$ for any real numbers A and B , we get

$$(\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(n))^2 \leq 2 \cdot (\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N))^2 + 2r^2 \log^2(2)$$

for $\sqrt{N} < n \leq N$. Hence the right-hand side in (8) is smaller than

$$o(1) + \frac{2}{\epsilon^2 \cdot (r \log \log(\sqrt{N}))^2} \cdot \frac{1}{N} \sum_{0 < n \leq N} (\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N))^2.$$

By the case $k = 2$ in theorem 1.3, one has

$$\frac{1}{N} \sum_{0 < n \leq N} (\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N))^2 \sim r \log \log(N), \quad N \rightarrow \infty.$$

Hence (7) holds and corollary 1.6 follows. \square

3.3. Proof of corollary 1.7. We shall need lemma 3.2 below whose proof is almost identical to the proof of corollary 1.6. The difference is that one applies theorem 1.3 with an arbitrary even integer k , in contrast to $k = 2$.

Set

$$I_k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^{2k} e^{\frac{-t^2}{2}} dt$$

for each positive integer k .

Lemma 3.2. *Let k be a positive integer. Then there exists some positive constant $A(k)$ such that*

$$\frac{|\{0 < n \leq N : |\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)| \geq C\}|}{N} \leq \frac{2I_k \cdot (r \log \log(N))^k}{C^{2k}}$$

for each positive integer $N \geq A(k)$ and every positive real number C .

Proof. Given a positive integer N and a positive real number C , let $S_{N,C}$ be the set of all integers $n \geq 1$ such that

$$|\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)| \geq C.$$

One has

$$\frac{1}{N} \sum_{\substack{0 < n \leq N \\ n \in S_{N,C}}} 1 \leq \frac{1}{N} \cdot \frac{1}{C^{2k}} \sum_{0 < n \leq N} (\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N))^{2k}.$$

By using the $2k$ -th moment given in theorem 1.3, we get

$$\frac{1}{N} \cdot \frac{1}{C^{2k}} \sum_{0 < n \leq N} (\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N))^{2k} = \frac{(r \log \log(N))^k}{C^{2k}} \cdot (I_k + o(1))$$

where the $o(1)$ depends only on k , thus ending the proof. \square

Proof of corollary 1.7. Given a positive integer N , denote by $f(N)$ the number of positive integers $n \leq N$ such that

$$\text{Ram}_{E/\mathbb{Q}(T)}(n) \leq C$$

and by $g(N)$ the number of positive integers $n \leq N$ such that

$$|\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)| \geq |C - r \log \log(N)|.$$

If N is sufficiently large (depending on k , C and r), then, by lemma 3.2, one has

$$f(N) \leq g(N) \leq N \cdot (r \log \log(N))^k \cdot \frac{2I_k}{(C - r \log \log(N))^{2k}},$$

as needed. \square

4. PROOF OF THEOREM 1.3

4.1. Proof of theorem 1.3 under an extra assumption. In this section, we prove:

Proposition 4.1. *Assume that the following condition holds:*

(*) $P_i(n) > 0$ for each $i \in \{1, \dots, r\}$ and each $n \geq 1$, where the $P_i(T)$'s are defined in (5).

Then theorem 1.3 holds.

We break the proof of proposition 4.1 into three parts.

4.1.1. *Approximation of $\text{Ram}_{E/\mathbb{Q}(T)}$ by prime divisor counting functions.* Below we describe the function $\text{Ram}_{E/\mathbb{Q}(T)}$ in terms of several prime divisor counting functions (lemma 4.4).

First, we need the following lemma which summarizes our use of the classical result about ramification in specializations alluded to in §1.4.

Given a prime number p , let v_p be the p -adic valuation over \mathbb{Q} and $\mathbb{Z}_{(p)}$ the localization of \mathbb{Z} at the prime ideal generated by p .

Lemma 4.2. *For each sufficiently large prime number p (depending on the extension $E/\mathbb{Q}(T)$) and each positive integer n which is not a branch point of $E/\mathbb{Q}(T)$, the following two conditions are equivalent:*

- (a) *p ramifies in the specialization E_n/\mathbb{Q} of $E/\mathbb{Q}(T)$ at n ,*
- (b) *there is a unique index $i \in \{1, \dots, r\}$ such that $v_p(P_i(n)) > 0$ and $e_i \nmid v_p(P_i(n))$, where the e_i 's and the $P_i(T)$'s are defined in (4) and (5).*

Proof. For each $i \in \{1, \dots, r\}$, let $m_i(T)$ be the irreducible polynomial of t_i over \mathbb{Q} , where the t_i 's are defined in (3). So $P_i(T) = b_i \cdot m_i(T)$ for each index $i \in \{1, \dots, r\}$.

Below we use the notion of meeting modulo a prime number p . Recall that t and t' in $\mathbb{P}^1(\overline{\mathbb{Q}})$ meet modulo p if there exist a number field F such that $t, t' \in \mathbb{P}^1(F)$ and a valuation v of F lying over v_p such that either $v(t) \geq 0$, $v(t') \geq 0$ and $v(t - t') > 0$ or $v(1/t) \geq 0$, $v(1/t') \geq 0$ and $v((1/t) - (1/t')) > 0$.

Pick a positive real number p_0 such that every prime number $p > p_0$ satisfies the following three conditions:

- (i) p does not divide $b_1 \cdots b_r$,
- (ii) t_i and $1/t_i$ are integral over $\mathbb{Z}_{(p)}$ for each index $i \in \{1, \dots, r\}$ ⁴,
- (iii) p is a good prime for $E/\mathbb{Q}(T)$ in the sense of [Leg14, definition 2.5] (in particular, two distinct branch points cannot meet modulo p).

Fix a prime $p > p_0$ and an integer $n \geq 1$ which is not a branch point. From condition (i), one has $v_p(P_i(n)) = v_p(m_i(n))$, $i \in \{1, \dots, r\}$.

First, assume that condition (b) holds for some $i \in \{1, \dots, r\}$. Then $v_p(m_i(n)) > 0$. By the first part of [Leg13, lemma 2.5], the integer n meets the branch point t_i modulo p . From the second part of the *Specialization Inertia Theorem* [Leg14, §2.2], conditions (ii) and (iii) and since $v_p(m_i(n))$ is not a multiple of e_i , the prime number p ramifies in the specialization E_n/\mathbb{Q} of $E/\mathbb{Q}(T)$ at n , as needed for (a).

Conversely, assume that p ramifies in E_n/\mathbb{Q} . From the first part of the *Specialization Inertia Theorem* and condition (iii), n meets some branch point (different from ∞) modulo p . By the definition of the set $\{t_1, \dots, t_r\}$ and by the second part of [Leg13, remark 2.3], there

⁴Condition (i) implies that t_1, \dots, t_r are integral over $\mathbb{Z}_{(p)}$.

is an $i \in \{1, \dots, r\}$ such that n and t_i meet modulo p . As p satisfies condition (ii), one may apply the second part of [Leg13, lemma 2.5] to get $v_p(P_i(n)) > 0$. Since n meets t_i modulo p and p satisfies conditions (ii) and (iii), one may apply the second part of the *Specialization Inertia Theorem* to get that the ramification index of each prime ideal lying over p in E_n/\mathbb{Q} is equal to $e' := e_i/\gcd(e_i, v_p(P_i(n)))$. As p ramifies in E_n/\mathbb{Q} , one has $e' > 1$, i.e. $v_p(P_i(n))$ is not a multiple of e_i .

It then remains to prove that an i as above is unique. Assume that condition (b) holds for two indices $i \neq j \in \{1, \dots, r\}$. In particular, one has $v_p(m_i(n)) > 0$ and $v_p(m_j(n)) > 0$. By the first part of [Leg13, lemma 2.5], n meets the two branch points t_i and t_j modulo p . Hence there is a σ in the absolute Galois group of \mathbb{Q} such that the branch points t_i and $\sigma(t_j)$ meet modulo p . As p satisfies condition (iii), one has $t_i = \sigma(t_j)$, which contradicts the definition of the set $\{t_1, \dots, t_r\}$. \square

Lemma 4.2 motivates the following definition.

Definition 4.3. Given two positive integers a and n , set

$$m_a(n) = |\{p : v_p(n) > 0 \text{ and } a|v_p(n)\}|.$$

In the special case $a = 1$, we retrieve the classical function ω , i.e. $\omega(n) = m_1(n)$ for each positive integer n .

In terms of definition 4.3, lemma 4.2 provides the following approximation of $\text{Ram}_{E/\mathbb{Q}(T)}$.

Lemma 4.4. *There exists some real number $C \geq 1$ such that*

$$\left| \text{Ram}_{E/\mathbb{Q}(T)}(n) - \omega(P_E(n)) + \sum_{i=1}^r m_{e_i}(P_i(n)) \right| \leq C$$

for each positive integer n which is not a branch point, where the polynomial $P_E(T)$ is defined in (6).

As condition (*) from proposition 4.1 holds, the integers $\omega(P_E(n))$ and $m_{e_i}(P_i(n))$, $1 \leq i \leq r$ and $n > 0$, are well-defined.

Proof. By lemma 4.2, there exists some real number $C \geq 1$ such that

$$(9) \quad \left| \text{Ram}_{E/\mathbb{Q}(T)}(n) - \sum_{i=1}^r \omega(P_i(n)) + \sum_{i=1}^r m_{e_i}(P_i(n)) \right| \leq C$$

for each positive integer n which is not a branch point.

Let n be a positive integer which is not a branch point, $i \neq j \in \{1, \dots, r\}$ and p a common prime divisor of $P_i(n)$ and $P_j(n)$. Assume that p satisfies both conditions (i) and (iii) from the proof of lemma 4.2. Then one has $v_p(P_i(n)/b_i) > 0$ and $v_p(P_j(n)/b_j) > 0$. As explained

in the last paragraph of the proof of lemma 4.2, this provides that the branch points t_i and t_j are conjugate over \mathbb{Q} , which cannot happen by the definition of the set $\{t_1, \dots, t_r\}$. Hence there exists some positive real number C' (not depending on n) such that

$$(10) \quad \left| \omega(P_E(n)) - \sum_{i=1}^r \omega(P_i(n)) \right| \leq C'.$$

It then remains to combine (9) and (10) to finish the proof. \square

4.1.2. *Estimating moments.* Let us start by estimating the moments of the functions m_a , $a \geq 2$.

Lemma 4.5. *Let a and k be two positive integers such that $a \geq 2$ and let $P(T) \in \mathbb{Z}[T]$ be a separable polynomial satisfying $P(n) > 0$ for each positive integer n . Then there exists some positive real number $C(P, k)$ such that*

$$\sum_{0 < n \leq N} m_a^k(P(n)) \leq C(P, k) \cdot N$$

for each positive integer N .

Note that lemma 4.5 fails in the case $a = 1$ since

$$\sum_{0 < n \leq N} \omega(n) \sim N \cdot \log \log(N)$$

as N tends to ∞ [HR17].

Proof. Let N be a positive integer. Since $a \geq 2$, one has

$$(11) \quad \sum_{0 < n \leq N} m_a^k(P(n)) \leq \sum_{0 < n \leq N} \left(\sum_{p^2 | P(n)} 1 \right)^k = \sum_{0 < n \leq N} \sum_{\substack{(p_1, \dots, p_k) \\ p_1^2 | P(n) \\ p_k^2 | \ddots P(n)}} 1.$$

Pick two positive real numbers α and β (depending only on the polynomial $P(T)$) such that $\sqrt{P(n)} \leq \alpha \cdot n^\beta$ for every positive integer n . By changing the order of summation in the right-hand side in (11), we get

$$(12) \quad \sum_{0 < n \leq N} m_a^k(P(n)) \leq \sum_{p_1 \leq \alpha \cdot N^\beta} \cdots \sum_{p_k \leq \alpha \cdot N^\beta} \sum_{\substack{0 < n \leq N \\ p_1^2 | P(n) \\ p_k^2 | \ddots P(n)}} 1.$$

Given a k -tuple $\underline{p} = (p_1, \dots, p_k)$ of prime numbers, let $S_{\underline{p}}$ be the set of distinct prime numbers appearing in \underline{p} and set $\Pi_{\underline{p}} = \prod_{p \in S_{\underline{p}}} p$. Then one has

$$(13) \quad \sum_{\substack{0 < n \leq N \\ p_1^2 | P(n) \\ \vdots \\ p_k^2 | \tilde{P}(n)}} 1 = \sum_{\substack{0 < n \leq N \\ \Pi_{\underline{p}}^2 | P(n)}} 1.$$

Next, for each positive integer M , let $\nu(M)$ be the number of integers $m \in \{0, \dots, M-1\}$ such that $P(m) \equiv 0 \pmod{M}$. Then

$$(14) \quad \sum_{\substack{0 < n \leq N \\ \Pi_{\underline{p}}^2 | P(n)}} 1 \leq \nu(\Pi_{\underline{p}}^2) \cdot \frac{N}{\Pi_{\underline{p}}^2}.$$

By the Chinese Remainder Theorem, one has

$$(15) \quad \nu(\Pi_{\underline{p}}^2) = \prod_{p \in S_{\underline{p}}} \nu(p^2).$$

Then, by (13), (14) and (15), we get

$$(16) \quad \sum_{\substack{0 < n \leq N \\ p_1^2 | P(n) \\ \vdots \\ p_k^2 | \tilde{P}(n)}} 1 \leq N \cdot \prod_{p \in S_{\underline{p}}} \frac{\nu(p^2)}{p^2}.$$

Now, combine (12) and (16) to get

$$\begin{aligned} \sum_{0 < n \leq N} m_a^k(P(n)) &\leq N \cdot \sum_{p_1 \leq \alpha \cdot N^\beta} \cdots \sum_{p_k \leq \alpha \cdot N^\beta} \prod_{p \in S_{\underline{p}}} \frac{\nu(p^2)}{p^2} \\ &\leq N \cdot \sum_{m=1}^k \binom{k}{m} \left(\sum_{p \leq \alpha \cdot N^\beta} \frac{\nu(p^2)}{p^2} \right)^m. \end{aligned}$$

As $\nu(p^2) \leq \deg(P)$ for each prime p not dividing the discriminant of $P(T)$, the inner series above is convergent, thus ending the proof. \square

Lemma 4.6. *For each positive integer k , there exists some positive constant $C(k)$ such that*

$$(17) \quad \left| \sum_{0 < n \leq N} \left(\text{Ram}_{E/\mathbb{Q}(T)}(n) - \omega(P_E(n)) \right)^k \right| \leq C(k) \cdot N$$

for each positive integer N .

Proof. For each integer $n \geq 1$ which is not a branch point, set

$$(18) \quad g(n) = \text{Ram}_{E/\mathbb{Q}(T)}(n) - \omega(P_E(n)) + \sum_{i=1}^r m_{e_i}(P_i(n)).$$

Denote the left-hand side in (17) by $f(N)$, $N \geq 1$. By (18), one has

$$(19) \quad f(N) \leq \sum_{0 < n \leq N} \sum_{m=0}^k |g(n)|^{k-m} \binom{k}{m} \left(\sum_{i=1}^r m_{e_i}(P_i(n)) \right)^m.$$

Pick a real number $C \geq 1$ (depending only on $E/\mathbb{Q}(T)$) such that $|g(n)| \leq C$ for each integer $n \geq 1$ (lemma 4.4). Then, by (19), we get

$$(20) \quad f(N) \leq (1 + C)^k \cdot \sum_{0 < n \leq N} \left(\sum_{i=1}^r m_{e_i}(P_i(n)) \right)^k.$$

By Hölder's inequality, one has

$$(21) \quad \left(\sum_{i=1}^r m_{e_i}(P_i(n)) \right)^k \leq r^{k-1} \cdot \sum_{i=1}^r m_{e_i}^k(P_i(n))$$

for each positive integer $n \leq N$. Then, combine (20) and (21) to get

$$f(N) \leq (1 + C)^k \cdot r^{k-1} \cdot \sum_{i=1}^r \sum_{0 < n \leq N} m_{e_i}^k(P_i(n)).$$

It then remains to apply lemma 4.5 to the polynomials $P_1(T), \dots, P_r(T)$ to finish the proof of lemma 4.6. \square

4.1.3. Conclusion. We can now complete the proof of proposition 4.1. As condition $(*)$ has been assumed to hold, we may apply [Hal56, theorem 1.4] and a classical result of Landau (see *e.g.* [SMC06, §XV.33, 1) b)]) to get

$$(22) \quad \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{0 < n \leq N} \left(\frac{\omega(P_E(n)) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{\frac{-t^2}{2}} dt$$

for each integer $k \geq 1$. It then remains to combine (22) and lemma 4.6 to finish the proof of proposition 4.1. \square

4.2. Proof of theorem 1.3. It suffices to show that condition $(*)$ from proposition 4.1 is redundant.

For each index $i \in \{1, \dots, r\}$, the leading coefficient b_i of the polynomial $P_i(T)$ has been assumed to be positive. Hence there exists some positive integer α such that $P_i(n + \alpha) > 0$ for each $i \in \{1, \dots, r\}$ and each positive integer n . Set $U = T - \alpha$. Then condition $(*)$ holds for the extension $E/\mathbb{Q}(U)$. Fix a positive integer k . Then proposition 4.1 gives that

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{0 < n \leq N} \left(\frac{\text{Ram}_{E/\mathbb{Q}(U)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{\frac{-t^2}{2}} dt.$$

For each positive integer n , the specialization of the extension $E/\mathbb{Q}(U)$ at n and the specialization of the extension $E/\mathbb{Q}(T)$ at $n + \alpha$ coincide. Hence one has

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{\alpha < n \leq N + \alpha} \left(\frac{\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{-\frac{t^2}{2}} dt.$$

One has

$$\sum_{0 < n \leq \alpha} \left(\frac{\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = O((\log \log(N))^{k/2}), \quad N \rightarrow \infty$$

and, by lemma 3.1, one has

$$\sum_{N < n \leq N + \alpha} \left(\frac{\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = O\left(\left(\frac{\log(N)}{\log \log(N)}\right)^k\right)$$

as N tends to ∞ . Hence

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{0 < n \leq N} \left(\frac{\text{Ram}_{E/\mathbb{Q}(T)}(n) - r \log \log(N)}{\sqrt{r \log \log(N)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{-\frac{t^2}{2}} dt,$$

as needed. \square

5. A FINAL REMARK ON THE NON GALOIS CASE

We conclude our paper by noticing that our results can easily be extended to the situation of arbitrary finite extensions of $\mathbb{Q}(T)$.

Let T be an indeterminate and $E/\mathbb{Q}(T)$ a finite extension (which is not necessarily Galois). Denote its Galois closure by $\hat{E}/\mathbb{Q}(T)$. Note that the sets of branch points of $E/\mathbb{Q}(T)$ and $\hat{E}/\mathbb{Q}(T)$ are the same.

First, we recall what are the specializations of $E/\mathbb{Q}(T)$. Fix a point $t_0 \in \mathbb{P}^1(\mathbb{Q})$ which is not a branch point of $\hat{E}/\mathbb{Q}(T)$. Denote the prime ideals lying over $(T - t_0)\overline{\mathbb{Q}}[T - t_0]$ in $E/\mathbb{Q}(T)$ by $\mathcal{P}_1, \dots, \mathcal{P}_s$. For each $l \in \{1, \dots, s\}$, the residue field at \mathcal{P}_l is denoted by $E_{t_0, l}$ and the extension $E_{t_0, l}/\mathbb{Q}$ is called a *specialization of $E/\mathbb{Q}(T)$ at t_0* . The *compositum* in $\overline{\mathbb{Q}}$ of the Galois closures of all specializations of the extension $E/\mathbb{Q}(T)$ at t_0 is the specialization of the Galois closure $\hat{E}/\mathbb{Q}(T)$ at t_0 .

Given an integer $n \geq 1$ which is not a branch point of $\hat{E}/\mathbb{Q}(T)$, let $\text{Ram}_{E/\mathbb{Q}(T)}(n)$ be the number of prime numbers p ramifying in some specialization $E_{n, l}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at n . As p ramifies in the *compositum* of finitely many extensions of \mathbb{Q} if and only if it ramifies in at least one of them (Abhyankar's lemma), we get $\text{Ram}_{E/\mathbb{Q}(T)} \equiv \text{Ram}_{\hat{E}/\mathbb{Q}(T)}$. Then theorems 1.3 and 1.4 as well as their corollaries extend to the non Galois case.

REFERENCES

- [Bec91] Sybilla Beckmann. On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.*, 419:27–53, 1991.
- [Bil95] Patrick Billingsley. *Probability and Measure*. Wiley Series in Probability and Mathematical Statistics. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1995. Third edition.
- [BSS] Lior Bary-Soroker and Tomer Schlank. On the minimal ramification problem, specializations, and prime values of polynomials. In preparation.
- [Hal56] H. Halberstam. On the distribution of additive number-theoretic functions. II. *J. London Math. Soc.*, 31:1–14, 1956.
- [HR17] G. H. Hardy and S. Ramanujan. The normal number of prime factors of a number n . *Quart. J. Math.*, 48:76–92, 1917.
- [JR03] John W. Jones and David P. Roberts. Septic fields with discriminant $\pm 2^a 3^b$. *Math. Comp.*, 72(244):1975–1985, 2003.
- [JR07] John W. Jones and David P. Roberts. Galois numbers fields with small root discriminant. *J. Number Theory*, 122(2):379–407, 2007.
- [Leg13] François Legrand. Specialization results and ramification conditions. 2013. Accepted for publication in Israel Journal of Mathematics. arXiv:1310.2189.
- [Leg14] François Legrand. Hilbert specialization results with local conditions. *Manuscript*, 2014. arXiv:1412.7635.
- [MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.
- [MR05] Gunter Malle and David Roberts. Number fields with discriminant $\pm 2^a 3^b$ and Galois group A_n or S_n . *LMS J. Comput. Math.*, 8:80–101, 2005.
- [Rob11] David P. Roberts. Nonsolvable polynomials with field discriminant 5^A . *Int. J. Number Theory*, 7(2):289–322, 2011.
- [Ser92] Jean-Pierre Serre. *Topics in Galois Theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992.
- [SMC06] József Sándor, Dragoslav S. Mitrinović, and Borislav Crstici. *Handbook of number theory. I*. Springer, Dordrecht, 2006. Second printing of the 1996 original.
- [Zyw13] David Zywina. The inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_p)$. *Manuscript*, 2013. arXiv:1303.3646.
- [Zyw14] David Zywina. The inverse Galois problem for orthogonal groups. *Manuscript*, 2014. arXiv:1409.1151.

E-mail address: barylior@post.tau.ac.il

SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, RAMAT AVIV,
TEL AVIV 6997801, ISRAEL

E-mail address: flegrand@post.tau.ac.il

SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, RAMAT AVIV,
TEL AVIV 6997801, ISRAEL

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, THE OPEN UNI-
VERSITY OF ISRAEL, RA'ANANA 4353701, ISRAEL